

CLAIMS

What is claimed is:

- 1 1. A method for managing network resources for externally authenticated users, the
2 method comprising:
3 authenticating a user in a first administrative domain;
4 generating a token for the user, the token assigning at least a first role for the user, the
5 first role identifying the user as a member of a pre-defined class of users; and
6 configuring the token to identify the user by the first role to a component of a second
7 domain.
- 1 2. The method of claim 1, wherein configuring the token to identify the user by the first
2 role includes configuring the token to identify the user as the first role to the
3 component of the second administrative domain without revealing a personal
4 identification of the user to the component.
- 1 3. The method of claim 1, wherein configuring the token to identify the user by the first
2 role includes configuring the token to identify the user by the first role to a policy
3 server external to the first administrative domain, thereby enabling the user to retrieve
4 network resources from the second administrative domain according to a policy of the
5 policy server.
- 1 4. A method as recited in claim 1,
2 wherein configuring the token to identify the user by the first role includes
3 configuring the token to identify the user by the first role to a policy server
4 external to the first administrative domain;
5 and further comprising the steps of:
6 receiving a request from the user to retrieve network resources from the second
7 administrative domain;

8 determining whether the user is authorized to access the network resources of the
 9 second administrative domain according to a policy of the policy server and
 10 based on the first role in the token.

1 5. The method of claim 1, wherein generating a token for the user includes assigning
 2 multiple roles for the user on the first token, each of the multiple roles being
 3 identifiable to a policy server external to the first administrative domain.

1 6. The method of claim 1, further comprising the steps of:
 2 attaching the token to a terminal associated with the user;
 3 automatically receiving the token at the second administrative domain when the user
 4 requests one or more resources from the second administrative domain.

1 7. The method of claim 1, further comprising the steps of:
 2 attaching an indicator for the token to a terminal associated with the user;
 3 automatically receiving the indicator to the component to inform the component of a
 4 location of the token on another computer.

1 8. The method of claim 1, wherein generating a token for the user includes providing
 2 information about a quality of authentication for the user.

1 9. The method of claim 1, wherein generating a token for the user includes providing
 2 information about a location of the user in the token.

1 10. The method of claim 1, wherein generating a token for the user includes providing
 2 information in the token about a personal identification of the user, a time stamp for
 3 when the token was generated, and the first role.

1 11. The method of claim 1, wherein generating a token for the user includes providing
 2 information in the token selected from a group of information consisting of
 3 information about a personal identification of the user, a time stamp for when the
 4 token was generated, and the first role; and further including the steps of encrypting at
 5 least some of the information in the token for use in the second administrative
 6 domain.

1 12. A method for managing network resources in multiple administrative domains, the
 2 method comprising:
 3 in a first administrative domain:
 4 authenticating a user in response to a request to access one or more
 5 resources in the first administrative domain;
 6 generating a token for the user, the token assigning at least a first role
 7 to the user, the first role identifying the user as a member of a class of users;
 8 in second administrative domain:
 9 receiving a second request from the user to access one or more second
 10 resources in the second administrative domain, wherein the second request
 11 includes the token;
 12 identifying a first policy for the first role specified by the token; and
 13 managing access of the user to the second resources according to the
 14 first policy.

1 13. The method of claim 12, wherein managing the user according to the first policy
 2 includes checking the first policy to determine if an operation requested by the user
 3 for the second resources of the second administrative domain is permitted for the first
 4 role.

- 1 14. The method of claim 12, wherein managing the user according to the first policy
2 includes checking the first policy to determine if access to the policy is permitted for
3 the first role, and wherein the method further comprises providing access to the user
4 for the second resources of the second administrative domain if the first policy
5 permits access to the second resources for any user assigned the role.
- 1 15. The method of claim 12, wherein managing the user according to the first policy
2 includes checking the first policy to determine if an operation requested by the user
3 for the second resources of the second administrative domain is permitted for the first
4 role, and wherein the method further comprises allowing execution of the operation
5 on the second resources only if the policy permits for the operation to be performed
6 by any user assigned the first role.
- 1 16. The method of claim 12, wherein managing the user according to the first policy
2 includes identifying a condition in which any user assigned the first role can access
3 the second resources of the second administrative domain, and wherein the method
4 further includes determining if the condition permits access to the second resources in
5 response to receiving a request from the user to access the second resources of the
6 second administrative domain.
- 1 17. The method of claim 12, wherein managing the user according to the first policy
2 includes identifying an allowable time period in which any user assigned the first role
3 can access the second resources of the second administrative domain, and wherein the
4 method further includes determining if the user is accessing the second resources of
5 the second administrative domain during the allowable time period
- 1 18. A method for managing network resources for externally authenticated users, the
2 method comprising:
3 receiving a first request to authenticate a user in a first administrative domain;

4 authenticating a user in a first administrative domain;
5 generating a token for the user, wherein the token includes information defining a first
6 role for the user, wherein the first role identifies the user as a member of a pre-
7 defined class of users;
8 receiving a second request from the user to access one or more network resources
9 located in a second administrative domain; and
10 determining whether to grant the user access to the network resources based on the
11 role in the token and without re-authenticating the user in the second
12 administrative domain.

1 19. A method for managing network resources in multiple administrative domains, the
2 method comprising:
3 assigning at least a first role to a plurality of users that access a first administrative domain;
4 and
5 causing each of the plurality of users to be identified by the first role on a component of the
6 second administrative domain, so that the first role identifies a policy that is shared by
7 the plurality of users for accessing resources managed in the second administrative
8 domain.

1 20. The method of claim 19, further comprising:
2 authenticating the plurality of users in a first administrative domain before assigning at least a
3 first role to the plurality of users.

1 21. The method of claim 19, further comprising assigning at least the first role to a
2 plurality of users during a network session between each of the users and the first
3 administrative domain, and causing each of the plurality of users to be identified by
4 the first role after each of the plurality of users selects to access the second
5 administrative domain during the network session.

1 22. The method of claim 19, wherein assigning at least a first role to a plurality of users
2 includes generating a token that identifies the first role to a policy server of the second
3 administrative domain.

1 23. A computer system for managing network resources, the computer system
2 comprising:
3 a storage medium that stores identification information for users that access the network;
4 processing resources located in a first administrative domain, the processing resources being
5 configured to:
6 access the storage medium to identify a user accessing the network;
7 generate a token for the user in response to the user accessing the network, the token
8 identifying at least a first role for the user; and
9 configure the token to enable the user to be identified by the first role in a second
10 administrative domain, so that the user is provided access to a resource of the
11 second administrative domain according to a policy for the first role.

1 24. The computer system of claim 23, wherein the processing resource is configured to
2 authenticate the user by accessing the identification information in the first storage
3 medium.

1 25. The computer system of claim 23, wherein the processing resources is configured to
2 associate the token with the user for a duration when the terminal of the user is
3 connected to the network.

1 26. The computer system of claim 23, wherein the token expires after the terminal is
2 disconnected from the network.

- 1 27. A computer system for managing network resources, the computer system
2 comprising:
3 a storage medium that stores identification information for users that access the network; and
4 processing resources located on a first administrative domain, the processing resource being
5 configured to:
6 access the storage medium to identify any one of a plurality of users that connect to a
7 network to access the first administrative domain;
8 generate a token for each user in the plurality of users in response to that user
9 accessing the network, the token identifying at least one of a plurality of role
10 for that user, the at least one of a plurality of role being concurrently
11 assignable to a plurality of other users;
12 associate the token with each user in the plurality of users so that subsequent access
13 by one of the plurality of users across the network to a network resource on a
14 second administrative domain is determined by the role identified by the
15 token.
- 1 28. The computer system of claim 27, wherein the processing resources are configured to
2 associate the token with each user in the plurality of users for a duration in which that
3 user is connected to the network.
- 1 29. The computer system of claim 27, wherein the processing resources are configured to
2 associate the token with each user in the plurality of users by attaching the token to a
3 terminal of each user, so that communications by that user automatically include the
4 token.

- 1 30. A computer-readable medium for managing network resources in multiple
2 administrative domains, the computer-readable medium carrying instructions for performing
3 the steps of:
4 assigning at least a first role to a plurality of users that access a first administrative domain;
5 and
6 causing each of the plurality of users to be identified by the first role on a component of the
7 second administrative domain, so that the first role identifies a policy that is shared by
8 the plurality of users for accessing resources managed in the second administrative
9 domain.
- 1 31. The computer-readable medium of claim 30, further comprising instructions for
2 authenticating the plurality of users in a first administrative domain before assigning
3 at least a first role to the plurality of users.
- 1 32. The computer-readable medium of claim 30, further comprising assigning at least the
2 first role to a plurality of users during a network session between each of the users and
3 the first administrative domain, and causing each of the plurality of users to be
4 identified by the first role after each of the plurality of users selects to access the
5 second administrative domain during the network session.
- 1 33. The computer-readable medium of claim 30, further comprising assigning at least a
2 first role to a plurality of users includes generating a token that identifies the first role
3 to a policy server of the second administrative domain.

- 1 34. A computer system for managing network resources in multiple administrative
2 domains, the computer system comprising:
3 in a first administrative domain:
4 means for authenticating a user that accesses the first administrative
5 domain from a terminal;
6 means for generating a token for the user, the token assigning at least a
7 first role to the user, the first role identifying the user as a member of a class of
8 users;
9 in second administrative domain:
10 means for receiving a communication from the user;
11 means for identifying a first policy for the first role specified by token;
12 and
13 means for managing the user according to the first policy.